

# Section C - Description/Specifications/Statement of Work

## Statement of Work (SOW)

### Division 51, Branch 514

#### DDG-51 FLTI, FLTII, FLTIIA, HED (Hybrid Electric Drive) Modernization and Obsolescence Machinery Control Systems Support

#### 1.0 INTRODUCTION

1.0.1. The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense entity responsible for research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles. This requirement is for NSWCPD Department 50, which supports FLT (Flight) I, FLTII, FLTIIA, HED (Hybrid Electric Drive), Modernization and Obsolescence Machinery Control Systems (MCS) DDG 51 Class ships.

1.0.2 This contract is for non-personal services. It does not create employment rights with the U.S. Government whether actual, inherent, or implied

#### 1.0.3 Government / Contractor Relationship

(a) The services to be delivered under this contract are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the task order between the Government and the Contractor's personnel. Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations.

(b) The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel. In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence

(c) Contractor personnel under this contract shall not engage in any of the inherently governmental functions listed at FAR Subpart 7.5 or DFARS Subpart 207.5.

#### (d) Employee Relationship:

1) The services to be performed under this contract do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.

2) Rules, regulations, directives, and requirements that are issued by the U. S. Navy and NSWCPD under its responsibility for good order, administration, security are applicable to all personnel who enter a Government installation or who travel on Government transportation. This is not to be construed interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

(e) Inapplicability of Employee Benefits: This contract does not create an employer-employee relationship. Accordingly, entitlements and benefits applicable to such relationships do not apply.

(f) Notice. It is the Contractor's, as well as the Government's, responsibility to monitor task order activities and notify the Contracting Officer if the Contractor believes that the intent of this Section has been or may be violated.

1) The Contractor should notify the Contracting Officer in writing within three (3) calendar days from the date of any incident that the Contractor considers constitute a violation of this Section. The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity of Government employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any communication involved in the conduct; and the estimate in time by which the Government must respond to this notice to minimize cost, delay, or disruption of performance.

2) The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer will either:

(i) Confirm the conduct is in violation and when necessary direct the mode of further performance,

(ii) Countermand any communication regarded as a violation,

(iii) Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or

(iv) In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which should be furnished by the Contractor.

## 1.2 SCOPE OF WORK

Naval surface ships require modernization-engineering, life-cycle, and in- service engineering support. This effort is to help ensure readiness and safety criteria is met. The work to be performed includes all activities such as Software development, Software deliveries, Software testing and Hardware Troubleshooting associated with FLTI, FLTH, FLTHA, Modernization, HED and Obsolescence Machinery Control Systems, computer program development, testing, equipment harvesting, and installation for ship construction. Tasks include performing systems engineering analysis in order to interface control systems with other new or modified shipboard systems; troubleshooting control systems hardware and software issues at the Land Based Engineering Site (LBES) or Test

Facilities in Philadelphia, PA, as well as sustainment and fleet modernization efforts around the world; upgrading the cyber security features of the existing and future control system variants; and addressing obsolete hardware with the most cost effective solutions possible.

## 2.0 APPLICABLE DOCUMENTS

- 2.1 DON-IT Acceptable Use Policy Memorandum, dated 12 FEB 2016
- 2.2 U.S. Navy Afloat Control Systems Cyber Security Classification Guide (10-040) Draft Rev 1
- 2.3 DoD Instruction 8510-01, Risk Management Framework
- 2.4 DoD 8570.01-M "Information Assurance Workforce Improvement Program"
- 2.5 DoD 8140.01 "Cyberspace Workforce Management requirement"

These documents will be sent separately.

The Contractor shall reference and utilize the latest version available when performing tasks within this SOW (Statement of Work).

## 3.0 REQUIREMENTS (CDRL A001)

**3.1 Machinery Control System (MCS) Computer Program Development:** To ensure the readiness and safety of FLTI, FLTH, FLTHA, Modernization, HED and Obsolescence of Navy Surface ships, NSWCPD is responsible for the software development and lifecycle support of the MCS computer programs shipboard and at Land Based Engineering Site (LBES). In support of this mission, the Contractor shall:

- 3.1.1 Provide software lifecycle support following the NSWCPD System Engineering Process (SEP) with applicable Capability Maturity Model Integrated (CMMI) and Institute of Electrical and Electronics Engineers (IEEE) standards and specifications.
- 3.1.2 Develop new and modified control system computer program modification from detailed requirements. Provide input to software team to develop requirements and desired functionality of the control system.
- 3.1.3 Develop and/or modify computer code in the following languages: C/C++, Java, C#, Visual Basic, MATLAB, and Simulink, as well as other related high level programming languages. The contractor will support a range of integrated developer environments including Visual Studio, Netbeans, and .NET Framework.
- 3.1.4 Develop and/or modify Graphical User Interfaces using applicable development tools.
- 3.1.5 Develop databases such as Microsoft Access and Structured Query Language (SQL)
- 3.1.6 Develop software for embedded systems.
- 3.1.7 Use networked and IP based systems and knowledge of network protocols including TCP/IP (Transmission Control Protocol/Internet Protocol) and UDP (User Datagram Protocol).
- 3.1.8 Develop and/or upgrade machinery plant simulations in order to enhance control system embedded trainer simulation system.
- 3.1.9 Develop software unit tests in order to demonstrate that the modified computer programs satisfy the requirements.
- 3.1.10 Develop software change packages and artifacts and present at peer reviews.
- 3.1.11 Use software issue reporting databases.

### **3.2 Machinery Control Systems Testing and Integration Engineering Services for FLTI, FLTII, FLTIIA, Modernization, HED and Obsolescence.**

The Contractor shall:

- 3.2.1 Develop, plan, schedule, and execute test plans and test procedures for individual MCS computer programs and MCS hardware.
- 3.2.2 Document issues, faults, or deficiencies found during software or hardware testing.
- 3.2.3 Provide remote troubleshooting assistance to onsite control system representatives who are supporting ship light off and installation activities.
- 3.2.4 Perform configuration management of control system software and documentation in accordance with the approved SEP Configuration Management Plan using software version control tools.
- 3.2.5 Provide hardware administration, maintenance, and disaster recovery support.
- 3.2.6 Provide Information Assurance (IA) support services to facilitate ongoing accreditation efforts.
- 3.2.7 Maintain technical software development skills to contribute to new software development efforts.
- 3.2.8 Develop software and hardware installation plans with input from Fleet, Type Commanders, Functional and Platform Program Managers, Planning Yards, Ship Management Representatives (SMR's), and external supporting commands and technical authorities.
- 3.2.9 Develop, maintain, and configuration manage software and hardware installation procedures, instructions, notices and Standard Operating Procedures.
- 3.2.10 Develop Ship Change Documents (SCD) packages for control system deliveries.
- 3.2.11 Develop Engineering Change Proposal (ECP) packages for control systems.
- 3.2.12 Provide engineering services that include development and maintenance in support of hardware and software technical documentation and requirements.
- 3.2.13 Provide engineering services that include development and maintenance in support of hardware shipboard installation technical data packages (TDP's).

**3.3 LBES/Test Facility Equipment Integration Support FLTI, FLTII, FLTIIA, Modernization (Back-Fit) and Obsolescence:** The LBES offers cost effective, risk mitigation solutions to test and provide integrated systems for operational effectiveness for DDG 51 Class vessels. In support of this mission, the Contractor shall:

- 3.3.1 Develop software programs for use in test tools and facility infrastructure tools based on customer requirements utilizing Java, C/C++, MATLAB, Simulink, Python, C#, and LabView.
- 3.3.2 Modify existing test tool/facility infrastructure tools to implement enhanced capability based on requirements.
- 3.3.3 Troubleshoot in-house systems to identify root cause of problems that are found in during software development and testing.
- 3.3.4 Develop equipment integration designs for networking, supervisory control systems, simulators/stimulators, and other test tools/systems developed in-house.
- 3.3.5 Develop/modify drawings, documentation, plans, and procedures for equipment integration and site upgrades.

**3.4 FLTI, FLTII, FLTIIA, Modernization, HED and Obsolescence Machinery Control Systems Integration with Other Ship Systems.** The contractor shall support MCS integration with the following systems: Electric Plant Systems, Propulsion Plant Systems, Data Multiplex Systems, Bridge and Navigation Systems, Integrated Condition Assessment System (ICAS), Digital Video Surveillance Systems (DVSS), Fuel Control System (FCS), Shipboard Networks, Auxiliary Control Systems, and Local machinery and damage control systems. The contractor shall support integration efforts as follows:

- 3.4.1 Improve existing communication interfaces or develop new interfaces between control systems and FLTIIA and FLTIII ship systems.
- 3.4.2 Development of technical documentation as it relates to control system or control system interfaces (e.g. Interface Design Documents, user manuals, training manuals, troubleshooting/maintenance guides).
- 3.4.3 Review technical information on new ship systems and document impacts.
- 3.4.4 Design human/machine (i.e. GUI's – primarily in Altia, C++, .NET) and machine/machine interfaces to support the integration of new ship systems.
- 3.4.5 Design and implement test tools (e.g. Sim/Stim, Emulators, Message Pumps) to support software development and integration testing of new ship systems with machinery control systems.

- 3.4.6 Provide remote and on-site troubleshooting and root cause analysis support for other ship systems interfaced to machinery control systems.
- 3.4.7 Design, implement, debug and test technical solutions in software (primarily C/C++, C++.net, C# and Java) to support the integration of new ship systems with MCS.
- 3.4.8 Configure and test software updates on land based test facilities in preparation for ship deliveries.
- 3.4.9 Maintain configuration control of documentation and software updates from vendors and other technical departments and provide analysis of any potential impacts that updates would have on machinery control systems.

### **3.5 Shipboard Troubleshooting, Test, and Installation FLTI, FLTH, FLTHA, HED and Modernization Ships**

- 3.5.1 Perform shipboard software loads on windows computers, VxWorks processors, PLC processors and cards, and circuit level firmware.
- 3.5.2 Repair various shipboard hardware and electronic equipment, such as cable harness wiring, cable harness routing, terminal box wiring, connector pinouts, wire splicing, equipment rack-in and rack-out, and cable terminations.
- 3.5.3 Perform troubleshooting on various electronic equipment such as computer hardware, computer operating systems, computer peripherals, various electronic sensors, terminal box wiring, cable wiring, electronic circuits, contact closure devices, and mechanical/electronic switches.
- 3.5.4 Provide shipboard installation, troubleshooting, and test assessment plans, routine status, metrics, and final trip reports.
- 3.5.5 Provide support for facilitating, preparing and tracking the shipment of Software Images and Hardware to and from the waterfront.
- 3.5.6 Assistance with identifying drawing discrepancies, configuration issues, equipment deficiencies, and special or operational interference.
- 3.5.7 Troubleshoot various Hull Mechanical & Electrical (HM&E) equipment to determine impact upon software development and maintenance.
- 3.5.8 Develop and maintain various software and equipment installation, equipment checkout, system troubleshooting and system assessment work products. The work products shall include the following: operational and endurance parameters, testing procedures, test plans, maintenance procedures, installation procedures, operational procedures, equipment installation drawings, equipment installation requirements, equipment removal packages, troubleshooting plans, troubleshooting guides, and pass/fail criteria.
- 3.5.9 Provide technical and engineering support during shipboard troubleshooting of control system problems.
- 3.5.10 Provide installation support for various cable types, connector types, transmitters, sensors, computer systems, wiring harnesses, wiring terminal boxes, and Human Machinery Interfaces (HMI).
- 3.5.11 Develop and present technical presentations and information to various entities such as peers, shipboard installation managers, ship's force representatives, and program sponsors.
- 3.5.12 Develop and maintain tracking sheets for various types of work products, including test equipment tracking, purchase order tracking, test procedure tracking, failed asset tracking, and equipment calibration tracking.
- 3.5.13 Provide shipboard operator and maintenance training of the control system.
- 3.5.14 Conduct control system test procedures during shipboard test evolutions.
- 3.5.15 Implement and track test failures and issues in the System Problem/Improvement Report (SPIR) database.
- 3.5.16 Provide administrative support for contracted employees who are travelling to remote locations. This includes submitting any access requests, Joint Personnel Adjudication System (JPAS) requests, country clearance requests, and other paperwork required for travel to the specific location.
- 3.5.17 Perform both LBES and Shipboard Test Plans.
- 3.5.18 Prepare both LBES and Shipboard Test Reports.

### **3.6 Integrated Logistics Support (ILS)**

The contractor shall:

- 3.6.1 Develop, evaluate, and provide feedback on technical documentation and other logistics products such as technical manuals, allowable parts lists, preventative maintenance cards, and engineering procedures.

- 3.6.2 Provide system redlines, drawings, equipment schematics, and placards.
- 3.6.3 Develop and generate inventory reports on OM&S (Operating Material and Supplies) inventory levels; inventory is in relation to this SOW only.
- 3.6.4 Provide support in accessing planning yard ILS repositories.

### **3.7 Material and Asset Support**

- 3.7.1 Maintain inventory management of incoming and outgoing material and assets.
- 3.7.2 Support shipping of material and assets required for supporting of tasks listed herein.
- 3.7.3 Provide support with fabricating and assembling material and assets required for supporting of tasks listed herein, including lab and shipboard control panels.
- 3.7.4 Provide support with staging (drawing material from inventory in accordance with designs) of material and assets required for supporting of tasks listed herein.

### **3.8 General Training Support**

- 3.8.1 Assist with development of course materials, auditing ongoing courses and providing input into curriculum development.
- 3.8.2 Assist Government activities in classroom training and instruction.
- 3.8.3 Provide On-The-Job Training (OJT) for Ship's force and Regional Maintenance Center (RMC) personnel.

### **3.9 Surveys and Assessments**

- 3.9.1 Conduct HM&E machinery and systems inspections and certifications when required and provide system reports (including deficiencies) to NSWCPD representative.
- 3.9.2 Perform system and equipment operability tests.
- 3.9.3 Provide Quality Assurance (QA) inspections and installation tracking of components.

### **3.10 Obsolescence Support**

- 3.10.1 As the DDG-51 and other Navy Surface ships age, obsolescence management is needed to keep the ships in working order. The obsolescence program identifies systems that are at or near end of life and develops solutions for them. In order to support this mission, contractors shall perform the following:
- 3.10.2 Obsolescence Project Management
- 3.10.3 The Obsolescence Project manager will be responsible for finding replacements for parts that are obsolete. If material is not available then they need to manufacture that can build to original part.
- 3.10.4 Support obsolescence projects from identification to solution
- 3.10.5 Assist in managing the business and engineering obsolescence concerns of various stakeholders, including finding replacement parts of obsolescence material and in some cases redesigning the material.
- 3.10.6 Develop technical plans and solutions for obsolescence problems. Update and maintain plan as project progresses.
- 3.10.7 Develop solutions to difficult problems with regard to balancing cost, need date, integration into existing systems, conflicting stakeholder desires, and other factors.
- 3.10.8 Develop time estimates and schedules for projects. Update and maintain schedule as project progresses.
- 3.10.9 Develop budget estimates for project material and manpower needs. Update and maintain budget as project progresses.

### **3.11 Cybersecurity and Information Assurance (IA).** The contractor shall provide the following services:

3.11.1 Provide technical services in support of delivering cyber-secure systems and solutions including the development and submittal of Risk Management Framework (RMF) risk assessments, implementation of DoD secure system configuration and hardening requirements identified in Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs), Assured Compliance Assessment Solution (ACAS) vulnerability assessments, anti-virus (AV) scanning, Standard Engineering Process (SEP) artifacts, and other supporting documentation required for certifying and maintaining afloat, RDT&E, and/or enterprise platforms.

3.11.2 Develop RMF Assess & Authorize (A&A) package documentation in accordance with DOD/NAVSEA directives, which includes the following components: Platform IT (PIT) Determination package documentation, System Categorization Form, Information System Continuous Monitoring Strategy (ISCM), Security Plan (SP), Step Concurrence forms, Plan of Actions and Milestones (POA&M), Security Assessment Plan (SAP), Security Assessment Report (SAR), Risk Assessment Report (RAR), Security Authorization Package, CYBERSAFE Certification, Package Endorsement Letters, and any additional administrative/technical resources required for submission.

3.11.3 Ensure RMF A&A package is submitted to the certification authority (CA) in sufficient time for review and operational cybersecurity risk recommendation to obtain Designated Accrediting Authority (DAA) authorization decision prior to operations or tests on a live network (i.e. LBES or shipboard).

3.11.4 The contractor shall develop, maintain, and execute all IA related tasks and duties in accordance with regulations to include the development and execution of DIACAP/RMF Program to Plan of Action and Milestone (POA&M) or Security Technical Implementation Guide (STIG).

3.11.5 In accordance with RMF, the contractor shall monitor and maintain the security posture of IT systems to include patching, implementing STIGs, analyzing network traffic, and applying new physical security measures.

3.11.6 Develop and/or test new and existing security features to be implemented into the control system operating environment and/or software.

### **3.12 Logistics Specialist Support**

Contractors shall:

3.12.1 Prepare both Shipboard and Land based test site (LBES) Test procedures.

3.12.2 Prepare Test Reports when testing has been completed.

3.12.3 Perform Data Collection and Statistical Analyses.

3.12.4 Interpret Command and Department Guidance.

3.12.5 Input and log shipping requests information into Navy ERP to initiate the shipping process (Enterprise Resource Planning)

### **3.13 Configuration Management Support**

The contractor shall provide the following services:

3.13.1 In accordance with locally established Quality Assurance (QA) configuration control practices, the contractor will implement and maintain proper configuration management of equipment, software, and documentation using processes compliant with Capability Maturity Model Integration (CMMI) Level 3.

3.13.2 The contractor shall implement configuration version control practices and processes (checkout/checkin, version number control, system/software baselines, merge, build, testing, and release) to software, hardware, requirements, firmware, images, technical manuals, test procedures, and support documentation.

The contractor shall provide configuration version control using locally established forms, templates, databases, and applications (GIT, Telelogic DOORS, Microsoft SharePoint, Excel, Word Access and Project).

### **3.14 Manufacturing Phase-Out or Discontinuation of Production, Diminishing Sources, and Obsolete Materials or Components**

3.14.1 The contractor shall notify the contracting officer immediately upon

determining the unavailability of obsolete materials or components. The contractor may recommend a solution to include the impact on the contract price and delivery. The contractor shall not initiate any item redesign or incur any additional costs without the express, written authorization of the contracting officer.

### **3.15 Parts Obsolescence**

3.15.1 The contractor shall establish and implement a parts obsolescence program. In the event that manufacturing phase-out or discontinuance of production of such items is contemplated, the contractor is required to notify the contracting officer and publish the discontinuance in the Government-Industry Data Exchange Program (GIDEP), where feasible; and to provide immediate advance notice of production phase-out to the Contracting Officer and Technical POCs.

## **4.0 DATA REQUIREMENTS**

### **4.1 Contract Status Report (CDRL A001)**

4.1.1 This report shall reflect both prime and Subcontractor data if applicable at the same level of detail.

4.1.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable the Government's approval must be received in writing from the COR within 5 business days before formal submission.

### **4.2 Travel Report (CDRL A002)**

4.2.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.2.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

### **4.3 Contractor's Personnel Roster (CDRL A003 )**

4.3.1 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is re COR. This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

### **4.4 Small Business Utilization Report (CDRL A004)**

4.4.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.4.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is re COR.

### **4.5 Systems Security Plan (CDRL A005)**

4.5.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.5.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is re COR.

### **4.6 Government Property Inventory Report (CDRL A006)**

4.6.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.6.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is re COR.

## **5.0 SECURITY REQUIREMENTS**

5.1 The Contractor is responsible for completing all required Government mandated training to maintain security and network access to government sites and IT systems to include but not limited to: Antiterrorism Level 1 Awareness; Records Management in the DON: Everyone's Responsibility; Training and Readiness: The Active Shooter; NAVSEA Introduction to Controlled Unclassified Information; Operations Security (OPSEC); NAVSEA Counterintelligence Training; Privacy and Personally Identifiable Information (PII) Awareness Training; NAVSEA Physical Security training and Cybersecurity 101 Training. Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract.

5.1.1 In accordance with SECNAV M-5510.30 Chapters 5 and 6, all Contractor personnel that require access to Department of Navy (DON) information systems and/or work on-site are designated Non-Critical Sensitive/IT-II positions, which require an open investigation or favorable adjudicated National Agency Check (NACLC) by the Defense Counterintelligence and Security Agency (DCSA). Investigations should be completed using the SF-86 Form and the SF-87 finger print card. An interim clearance can be granted by the company Security Officer and recorded in the Joint Personnel Adjudication System (JPAS). An open or closed investigation with a favorable adjudication is required prior to issuance of a badge providing access to NSWCPD sites and buildings. If an unfavorable adjudication is determined by DCSA all access will be terminated. For Common Access Card (CAC) card you must have a completed investigation that has been favorably adjudicated or a final security clearance. A CAC Card will not be issued to contractors who have an interim security clearance.

## 5.2 On-Site Work

5.2.1 Contractor personnel that require a badge to work on-site at one of the NSWCPD sites must provide an I-9 form to verify proof of citizenship. The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship. Finally, contractors shall supply a copy of their OPSEC Training Certificate or other proof that the training has been completed.

5.2.2 Construction badges for contractor personnel that work on-site at one of the NSWCPD sites will be good for 60 days.

## 5.3 DD 254 Requirement

5.3.1 A Facility Access Determination (FAD) will be completed on any contractor that does not have a favorable adjudicated investigation in JPAS and is requesting swipe/non-swipe access to our buildings in excess of 120 days. Any contractor that has unfavorable information that has not been favorably adjudicated by Department of Defense Central Adjudication Facility (DOD CAF) will not be issued a badge.

5.3.2 The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-M), and (3) assure compliance with any written instructions from the NSWCPD, Security Office.

5.3.3 The Prime Contractor shall:

- 5.7.1 Forward signed copies of DD254s provided to subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: S
- 5.7.2 Direct the subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the prime Contractor.
- 5.7.3 Submit the subcontractor request for public release through the technical point of contact identified on the DD 254.

An Active SECRET Facility Clearance (FCL) is required for performance on this contract. There is no safeguarding requirement required.

Item 1(a): "All contractor personnel accessing classified information or material associated with and/or performing work relative to the resultant contract must be United States citizens and shall have and maintain at a minimum SECRET security clearance at time of contract award.

Note: classified and/or unclassified material which is marked : "not releasable to foreign nations" (NOFORN or NF) may not be released in any form to foreign governments, foreign nations, non-U.S. citizens or anyone representing a foreign government or foreign private interest without the permission of the Originator.

Contractor must comply with FAR clause 52.204-2 entitled "security requirements and national industrial Security program operating manual (NISPOM) in administering security matters incidental to the Performance of the requirements of the contract.

Item 10 (j). – The contractor shall provide adequate physical protection to the unclassified (for official use only) Information so as to preclude access by person or entity not authorized by the U.S. Government. DoD M-5200.01 Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI) of 2/24/2012.

Item 11 (a). – Contract performance is restricted to NSWC Philadelphia Division and other designated Navy and Department of Defense locations necessary to execute individual delivery orders.

Item 11(e) - Engineering Services: This contract is for engineering and technical support services for Code 523/Division 52 at the Naval Surface Warfare Center Philadelphia Division and/or its associated cleared facilities. Classification markings on the material to be furnished will provide the classification guidance necessary for performance of this contract.

-Classified or unclassified technical papers to be presented at a classified symposium must be approved by the NSWCPD Contracting Officer's Representative (COR) prior to the presentation.

-Security classification guides and controlled unclassified information (CUI) (e.g., FOUO, distribution statement controlled) are not authorized for public release; therefore, they cannot be posted on a publicly accessible web-server or transmitted over the internet unless appropriately encrypted. Request

public release cannot be transmitted via the internet until the contractor receives final approval from NSWCPD .

5.3.4 The planned utilization of non-U.S. Citizens in the performance of this contract effort must be identified by name and country of citizenship in the proposal. Foreign Nationals shall not be allowed access to classified or critical program information unless approved on a case by case basis by DSS.

5.3.5 The planned utilization of non-U.S. Citizens in the performance of this contract effort must be identified by name and country of citizenship in the proposal. Foreign Nationals shall not be allowed access to classified or critical program information unless approved on a case by case basis by DSS.

## **5.4 OPERATIONS SECURITY (OPSEC)**

**5.4.1** The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure. The NSWCPD Philadelphia Division's (NSWCPD) Critical Information List (CIL)/ CIIL (Critical Indicators and information list) will be provided on site, if warranted. Performance under this contract requires the contractor to adhere to OPSEC requirements. The Contractor may not impose OPSEC requirements on its subcontractors unless NSWCPD approves the OPSEC requirements. During the period of this contract, the Contractor may be exposed to, use, or produce, NSWCPD Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. NSWCPD's CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI).

**5.4.2** CUI correspondence transmitted internally on the contractor's unclassified networks or information systems, and externally, shall be protected per NIST SP-800-171, Protecting Controlled Unclassified Information (CUI) in Non-federal Systems and Organizations.

Assembled large components/systems being transported to and from testing areas, other production or government facilities (whether or not on public roadways) shall be in an enclosed van trailer or covered flatbed trailer. Component/System outside storage, staging, and test areas shall be shielded/obscured from public view wherever physically possible.

**5.4.3** NSWCPD's CI shall not be publicized in corporate wide newsletters, trade magazines, displays, intranet pages or public facing websites. Media requests related to this project shall be directed to the PCO, and the COR who will forward the request to the NSWCPD Public Release Authority for review.

**5.4.4** Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss/compromise of government Classified or CI, Business Sensitive, Company Proprietary information related to this or other program must be immediately reported to the contractor's Facility Security Officer and Cognizant Security Office and/or the Naval Criminal Investigative Service, and the NSWCPD Security Division (Code 105.1). Questions concerning these requirements shall be directed to the PCO, and the COR who will forward the request to the NSWCPD Security Division (Code 105.1).

## **5.5 RECEIPT, STORAGE, AND GENERATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

All Controlled Unclassified Information (CUI) associated with this contract must follow the minimum marking requirements of DoDI 5200.48, Section 3, paragraph 3.4.a, and include the acronym "CUI" in the banner and footer of the document. In accordance with DoDI 5200.48, CUI must be safeguarded to prevent Unauthorized Disclosure (UD). CUI export controlled technical information or other scientific, technical, and engineering information must be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR. Nonfederal information systems storing and processing CUI shall be protected per NIST SP-800-171, or subsequent revisions. All transmissions to personal email accounts (AOL, Yahoo, Hotmail, Comcast, etc.) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc.) are prohibited. Destroy CUI associated with this contract by any of the following approved methods: A cross-cut shredder; a certified commercial destruction vendor; a central destruction facility; incineration; chemical decomposition; pulverizing, disintegration; or methods approved for classified destruction.

## **5.7 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING**

### **5.7.1 System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews**

**5.7.1.1** Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.

**5.7.1.2** If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

**5.7.1.3** Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP(s).

**5.7.1.4** The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

### **5.10.2 Compliance to NIST 800-171**

5.10.2.1 The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.

5.10.2.2 Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

5.10.2.3 Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

5.10.2.4 Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

5.10.2.5 Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

5.10.2.6 Audit user privileges on at least an annual basis;

5.10.2.7 Implement:

5.10.2.7.1 Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,

5.10.2.7.2 NIST Cryptographic Algorithm Validation Program (CAVP) (see <https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program>);

5.10.2.8 Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

5.10.2.9 Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

### **5.10.3 Cyber Incident Response:**

5.10.3.1 The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

5.10.3.2 Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at [http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions\\_for\\_Submitting\\_Media.docx](http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx). In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

5.10.3.3 If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

### **5.10.4 Naval Criminal Investigative Service (NCIS) Outreach**

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

### **5.10.5 NCIS/Industry Monitoring**

5.10.5.1

In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the Naval Criminal Investigative Service (NCIS), which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

#### 5.10.5.2

If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of an alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.

#### 5.10.5.3

In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and local law.

### 6.0 PLACE OF PERFORMANCE

6.1 The primary place of performance shall be at NSWCPD in Philadelphia. Travel may be required to the locations listed in Section 7.0.

6.1.1 The specific location(s) will be provided at time of award of the task order. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

6.1.2 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this task order. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

#### 6.1.3 Early Dismissal and Closure of Government Facilities

When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the contract for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the task order. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the task order period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allowability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

### 7.0 TRAVEL

7.1 The Contractor may be required to travel from the primary performance location when supporting this requirement.

The contractor shall be required to travel CONUS (any state in USA) and OCONUS (primarily Japan, and any country in Europe) to accomplish the tasks contained in this contract. Travel in support of this requirement is anticipated to include, but may not be limited to, the following alternate performance locations (per year):

CONUS/OCONUS	ORIGIN	DESTINATION	Number of Trips	Number of people
CONUS	Philadelphia	Washington, D.C.	1	1
CONUS	Philadelphia	Norfolk, VA	8	2
CONUS	Philadelphia	San Diego, CA	10	2
CONUS	Philadelphia	Everett, WA	2	2
OCONUS	Philadelphia	Yokosuka, Japan	4	2
CONUS	Philadelphia	Mayport, FL	2	2
CONUS	Philadelphia	Pascagoula, MS	1	2
CONUS	Philadelphia	Bath, ME	2	2
CONUS	Philadelphia	Honolulu, HI	3	2
OCONUS	Philadelphia	Rota, Spain	2	2
CONUS	Philadelphia	Orlando, FL	1	1
CONUS	Philadelphia	Annapolis, MD	1	1
CONUS	Philadelphia	Leesburg, VA	1	1
CONUS	Philadelphia	New Orleans, LA	1	1
CONUS	Philadelphia	Milwaukee, WI	1	1
CONUS	Philadelphia	Cincinnati, OH	1	1

MOD P0006 has added the following travel location under TI-01 REV 1:

CONUS/OCONUS	ORIGIN	DESTINATION	Number of Trips	Number of people
CONUS	Philadelphia	Portland, OR	1	1

MOD P0010 has added the following travel locations under TI's 02 & 03

CONUS/OCONUS	Origin	Destination	Duration of Trip	# of Trips	# of People
CONUS	Philadelphia	Johnstown, PA	7 days	2	1
CONUS	Philadelphia	Fort Collins, CO	7 days	2	1

7.2 The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved by the COR before travel occurs. Approval may be via the Technical Instruction (TI). In accordance with the TI instructions, before initiating any travel the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice

7.3 All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 Travel Cost (NAVSEA) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002).

#### 7.4 Travel Costs

7.4.1 The current "maximum per diem" rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

The Contractor will be required to travel to CONUS and OCONUS destinations, duration, and number of trips are subject to change; Washington, DC, Norfolk, VA, San Diego, CA, Everett, WA, Yokosuka, Japan, Mayport, FL, Pascagoula, MS, Bath, ME, Honolulu, HI, Rota, Spain, Orlando, FL, New Orleans, LA, Milwaukee, WI, Cincinnati, OH, Leesburg, VA, Annapolis, MD, Great Lakes, IL.

## 8.0 PURCHASES

8.1 Only items directly used and incidental to the services for this Contract/Task Order and for work within the scope of the Statement of Work/Performance Work statement shall be purchased under the Other Direct Cost (ODC) line items. Purchases of an individual item that is valued above \$10,000 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR) it shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing. Provide copies of price estimates from at least 2 vendors.

8.2 Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under this Contract/Task Order shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

## 9.0 PERSONNEL

9.1 Personnel Requirements. All persons proposed in key and non-key labor categories shall, at the time of proposal submission, be U.S. citizens holding at least a current SECRET clearance, or possess a favorable DCSA adjudication as outlined in section 5.0.

9.2 Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state "zero" if not approved. If overtime premium has not been approved under this contract in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime contractor. This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully-burdened premium OT labor costs

9.3 The level of effort for the performance of the resultant Contract/Task Order is based on the following labor categories and hours per year:

#### Base Year

<u>Title (Key Personnel)</u>	Site	Hours	OT HRs	Resumes Req
------------------------------	------	-------	--------	-------------

ENGINEER, SYSTEMS IV *	Government	3840	384	2
MANAGER, PROGRAM/PROJECT II*	Contractor	450	45	1
<b><u>Title (Non-Key Personnel)</u></b>				
COMPUTER PROGRAMMER IV	Government	3840	384	0
TECHNICIAN, ENGINEERING VI	Government	3840	384	0
ENGINEER, COMPUTER II	Government	1920	192	0
ENGINEER, COMPUTER IV	Government	3840	384	0
ANALYST, COMPUTER SYSTEMS III	Government	1920	192	0
COMPUTER PROGRAMMER II	Government	3840	384	0
ENGINEER, SYSTEMS I	Government	3840	384	0
ANALYST, MANAGEMENT II	Government	1920	192	0
TECHNICIAN, ENGINEERING III	Government	1920	384	0
SPECIALIST, CONFIGURATION MGMT I	Government	1920	192	0
SPECIALIST INFORMATION SYSTEM SECURITY II	Government	1920	192	0
ANALYST, COMPUTER SYSTEMS II	Government	1920	192	0
ADMINISTRATIVE ASSISTANT	Contractor	270	0	0

\* indicates key personnel

#### Option Year 1

<b><u>Title (Key Personnel)</u></b>	<b>Site</b>	<b>Hours</b>	<b>OT HRs</b>	<b>Resumes Req</b>
ENGINEER, SYSTEMS IV *	Government	3840	384	2

MANAGER, PROGRAM/PROJECT II*	Contractor	450	45	1
<b><u>Title (Non-Key Personnel)</u></b>				
COMPUTER PROGRAMMER IV	Government	3840	384	0
TECHNICIAN, ENGINEERING VI	Government	3840	384	0
ENGINEER, COMPUTER II	Government	1920	192	0
ENGINEER, COMPUTER IV	Government	3840	384	0
ANALYST, COMPUTER SYSTEMS III	Government	1920	192	0
COMPUTER PROGRAMMER II	Government	3840	384	0
ENGINEER, SYSTEMS I	Government	3840	384	0
ANALYST, MANAGEMENT II	Government	1920	192	0
TECHNICIAN, ENGINEERING III	Government	1920	384	0
SPECIALIST, CONFIGURATION MGMT I	Government	1920	192	0
SPECIALIST INFORMATION SYSTEM SECURITY II	Government	1920	192	0
ANALYST, COMPUTER SYSTEMS II	Government	3840	384	0
ADMINISTRATIVE ASSISTANT	Contractor	270	0	0

\* indicates key personnel

#### Option Year 2

<b><u>Title (Key Personnel)</u></b>	<b>Site</b>	<b>Hours</b>	<b>OT HRs</b>	<b>Resumes Req</b>
ENGINEER, SYSTEMS IV *	Government	3840	384	2

MANAGER, PROGRAM/PROJECT II*	Contractor	450	45	1
<b><u>Title (Non-Key Personnel)</u></b>				
COMPUTER PROGRAMMER IV	Government	3840	384	0
TECHNICIAN, ENGINEERING VI	Government	3840	384	0
ENGINEER, COMPUTER II	Government	1920	192	0
ENGINEER, COMPUTER IV	Government	3840	384	0
ANALYST, COMPUTER SYSTEMS III	Government	1920	192	0
COMPUTER PROGRAMMER II	Government	3840	384	0
ENGINEER, SYSTEMS I	Government	3840	384	0
ANALYST, MANAGEMENT II	Government	1920	192	0
TECHNICIAN, ENGINEERING III	Government	1920	384	0
SPECIALIST, CONFIGURATION MGMT I	Government	1920	192	0
SPECIALIST INFORMATION SYSTEM SECURITY II	Government	1920	192	0
ANALYST, COMPUTER SYSTEMS II	Government	3840	384	0
ADMINISTRATIVE ASSISTANT	Contractor	270	0	0

\* indicates key personnel

### Option Year 3

<b><u>Title (Key Personnel)</u></b>	<b>Site</b>	<b>Hours</b>	<b>OT HRs</b>	<b>Resumes Req</b>
ENGINEER, SYSTEMS IV *	Government	3840	384	2
MANAGER, PROGRAM/PROJECT II*	Contractor	450	45	1

<b><u>Title (Non-Key Personnel)</u></b>				
COMPUTER PROGRAMMER IV	Government	3840	384	0
TECHNICIAN, ENGINEERING VI	Government	3840	384	0
ENGINEER, COMPUTER II	Government	3840	384	0
ENGINEER, COMPUTER IV	Government	3840	384	0
ANALYST, COMPUTER SYSTEMS III	Government	1920	192	0
COMPUTER PROGRAMMER II	Government	3840	384	0
ENGINEER, SYSTEMS I	Government	3840	384	0
ANALYST, MANAGEMENT II	Government	1920	192	0
TECHNICIAN, ENGINEERING III	Government	1920	384	0
SPECIALIST, CONFIGURATION MGMT I	Government	1920	192	0
SPECIALIST INFORMATION SYSTEM SECURITY II	Government	1920	192	0
ANALYST, COMPUTER SYSTEMS II	Government	3840	384	0
ADMINISTRATIVE ASSISTANT	Contractor	270	0	0

\* indicates key personnel

#### Option Year 4

<b><u>Title (Key Personnel)</u></b>	<b>Site</b>	<b>Hours</b>	<b>OT HRs</b>	<b>Resumes Req</b>
ENGINEER, SYSTEMS IV *	Government	3840	384	2
MANAGER, PROGRAM/PROJECT II*	Contractor	450	45	1
<b><u>Title (Non-Key Personnel)</u></b>				

COMPUTER PROGRAMMER IV	Government	3840	384	0
TECHNICIAN, ENGINEERING VI	Government	3840	384	0
ENGINEER, COMPUTER II	Government	1920	192	0
ENGINEER, COMPUTER IV	Government	3840	384	0
ANALYST, COMPUTER SYSTEMS III	Government	1920	192	0
COMPUTER PROGRAMMER II	Government	3840	384	0
ENGINEER, SYSTEMS I	Government	3840	384	0
ANALYST, MANAGEMENT II	Government	1920	192	0
TECHNICIAN, ENGINEERING III	Government	1920	384	0
SPECIALIST, CONFIGURATION MGMT I	Government	1920	192	0
SPECIALIST INFORMATION SYSTEM SECURITY II	Government	1920	192	0
ANALYST, COMPUTER SYSTEMS II	Government	1920	192	0
ADMINISTRATIVE ASSISTANT	Contractor	270	0	0

\* indicates key personnel

## **9.4 Key Personnel**

9.4.1. The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this Contract/Task Order in accordance with Clause 52.237-3 Continuity of Services (Jan 1991) in the basic SeaPort contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

9.4.2. In accordance with C-237-H002 Substitution of Key Personnel, the following labor categories are designated as the target Key Personnel for this contract. Resumes will be submitted for each category in the quantities indicated by the key category description. Target qualifications are listed below for each education and work experience qualifications for each key personnel labor category. The proposed combined expertise of all proposed key personnel shall cover at a minimum all requirements for task areas (3.1, 3.2, 3.3, 3.4 & 3.5) in the performance work statement.

9.4.3. The Contractor shall provide individuals to fill the key positions identified below.

9.4.4. The Contractor shall indicate within the personnel section of its proposal, and/or indicate within individual submitted resume(s), any personnel security clearance requirements as stipulated in section 12.1 above.

The Contractor shall provide individuals to fill the key positions identified below:

**ENGINEER, SYSTEMS IV (ESY4) (two resumes required):**

**Minimum Education:** Bachelor of Science (BS) Degree in Electrical Engineering or Computer Engineering from an accredited college or university.

**Target Experience:**

- Five (5) years of professional experience within industry as a systems, electrical, and/or electronics engineer, which includes:
- Two (2) years of professional experience within industry acting as a lead engineer
- Three (3) years of professional experience troubleshooting hardware/software systems
- One (1) year of professional experience reading electrical schematics
- One (1) year of professional experience troubleshooting network based systems

**MANAGER, PROGRAM/PROJECT II (MANP2) (one resume required)**

Program Managers are concerned with the overall planning, direction and success of major programs, systems development efforts, and research or technology initiatives which have great significance to the activity's and agency's needs. Programs are typically large, multi-year efforts divided into several sub-programs/tasks. Establishment and control of technical milestones, schedules, budgets and costs are also essential tasks for the Program Manager. Working knowledge of the Naval Sea System Command, Naval Surface Warfare Center and Fleet organizations is desired.

**Minimum Education:** Bachelor's level degree in any technical or managerial discipline. In lieu of the education requirement, individuals should have fifteen (15) years of relevant experience in the program management and program oversight of Control System/Information System or other technical equipment, systems or programs for the U.S. Navy.

**Target Experience:** 10 years professional experience in program/project management.

**9.5 Non-Key Personnel**

Although resumes for "Non-Key Personnel" are not required, offerors must fully demonstrate their ability to provide the non-key personnel listed below who meet the requirements that follow. The contractor shall certify in their proposal that they have these non-key personnel and provide a statement as to their ability to supply the personnel with the experience required to perform the efforts specified in the performance work statement. The contractor shall provide individuals to fill the non-key positions identified below:

**COMPUTER PROGRAMMER IV(14074) (one resumes required):**

**Minimum Education:** Bachelor of Science degree in Computer Science, Electrical Engineering, or Computer Engineering from an accredited college or university

**Minimum Experience:**

- Seven (7) years of professional experience in software development in engineering and/or control systems, which includes:
- Two (2) years of professional experience using Microsoft Visual Studio to develop, compile, and debug source code for .NET Framework projects in C++/CLI, Managed C++, or C#
- One (1) year of professional experience as a technical and/or programming lead for a software project through the software life cycle, including the writing, reviewing, and maintaining new or existing software requirements, generating technical documentation regarding software, designing and analyzing software architectures, software configuration management, software implementation, product deployment, and planning and executing software maintenance activities
- One (1) year of professional experience supporting and troubleshooting networked, IP-based systems both locally and via distance support demonstrating a working knowledge and familiarity of network protocols such as TCP/IP and UDP

**TECHNICIAN, ENGINEERING VI (30086) (one resumes required):**

**Minimum Education:** High School Diploma or Trade/Industrial School Diploma (or GED Equivalent) and/or related military experience

**Minimum Experience:**

-Seven (7) years of professional experience as an Engineering Technician, which includes:

-Five (5) years of professional experience troubleshooting and tracing signals using electrical schematics and a digital multimeter to diagnose or isolate cause for electrical failures, then generating write ups that detail testing performed, troubleshooting steps, and findings.

-Two (2) years of professional experience within industry acting as a lead engineering technician

-Two (2) years of professional experience with personal computer file and directory structures as well as manipulating computer peripheral settings for use in desired applications

-

#### **ENGINEER, COMPUTER IV(EC4):**

**Minimum Education:** Bachelor of Science (BS) Degree in Electrical Engineering or Computer Engineering from an accredited college or university.

#### **MinimumExperience:**

-Ten (10) years of professional experience within industry as a systems, electrical, computer and/or electronics engineer, which includes:

-Two (2) years of professional experience within industry acting as a lead engineer

-Two (2) years of professional experience using LABVIEW and MATLAB/SIMULINK

-One (1) year of professional experience developing custom circuit board designs (PCB's) for use in integrated systems

#### **Engineer, Computer II (EC2):**

**Minimum Education:** Bachelor of Science (BS) Degree in Electrical Engineering or Computer Engineering from an accredited college or university

#### **Minimum Experience:**

-One (1) year of professional experience within industry as a systems, electrical, computer, and/or electronics engineer

-One (1) year of professional experience coding in C++

-One (1) year of professional experience coding in Java

-One (1) year of professional experience reading electrical schematics

-One (1) year of professional experience working with hardware/software systems

#### **Analyst, Computer Systems III (14103):**

**Minimum Education:** Bachelor of Science degree in Computer Science, Electrical Engineering, or Computer Engineering, or a Cyber Security related degree from an accredited college or university

#### **Minimum Experience:**

-Four (4) years of professional experience in cyber security engineering, which includes:

-Security+ and CISSP Certifications

-One (1) year of professional experience with IT infrastructure, networks, and/or network security involving the use of vulnerability analysis tools and the implementation and configuration of cyber security controls such as intrusion detection systems, intrusion prevention system, firewall configurations, and access control lists

-One (1) year of professional experience maintaining and configuring various operating systems such as Windows, Linux, VxWorks, or other Embedded Operating Systems

-One (1) year of professional experience writing, reviewing, and maintaining new or existing cyber security requirements

-

#### **Engineer, Systems I (ESY1):**

**Minimum Education:** Bachelor of Science (BS) Degree in Electrical Engineering from an accredited college or university.

**Minimum Experience:**

- One (1) year of professional experience within industry as a systems, electrical, and/or electronics engineer
- One (1) year of professional experience troubleshooting hardware/software systems
- One (1) year of professional experience reading electrical schematics
- One (1) year of professional experience troubleshooting network based systems

**Computer Programmer II (14072):**

**Minimum Education:** Bachelor of Science degree in Computer Science, Electrical Engineering, or Computer Engineering from an accredited college or university

**Minimum Experience:**

- Two (2) years of professional experience in software development in engineering and/or control systems using C++
- One (1) year of professional experience in software development using the Microsoft .NET framework
- One (1) year of professional experience using Microsoft Visual Studio to develop, compile, and debug source code in C++/CLI, Managed C++, or C#

**Analyst, Computer Systems II (14102):**

**Minimum Education:** Bachelor of Science degree in Computer Science, Electrical Engineering, or Computer Engineering or a Cyber Security related degree from an accredited college or university

**Minimum Experience:**

- Two (2) years of professional experience in cyber security engineering
- Security+ Certification or CISSP Certification
- One (1) year of professional experience with vulnerability analysis tools
- One (1) year of professional experience maintaining and configuring various operating systems such as Windows, Linux, VxWorks, or other Embedded Operating Systems

-

**ANALYST, MANAGEMENT II**

**Minimum Education:** High School Diploma or Trade/Industrial School Diploma (or GED Equivalent) and/or related military experience

**Minimum Experience:**

- One (1) year of professional experience in inventory management

**Technician, Engineering III (30083):**

**Minimum Education:** High School Diploma or Trade/Industrial School Diploma (or GED Equivalent) and/or related military experience

**Minimum Experience:**

- Two (2) years of professional experience as an Engineering Technician
- One year (1) of professional experience tracing signals and diagnosing or isolating cause for electrical failures
- One (1) year of professional experience reading, understanding, and interpreting electrical schematics

- One (1) year of professional experience generating write ups that detail testing performed, troubleshooting steps, and findings
- One (1) year of professional experience using a digital multimeter to conduct troubleshooting hardware systems
- One (1) year of professional experience using a personal computer to conduct troubleshooting and complete work product tasks
- 

#### **Specialist, Configuration Mgmt 1 (SCM1):**

**Minimum Education:** Bachelor's Degree in Science, Technology, Engineering, or Mathematics from an accredited college or university.

#### **Minimum Experience:**

- Two (2) years as a Configuration Manager
- One (1) year experience with requirements management using DOORS
- One (1) year experience with software configuration management specifically as it relates to libraries of multiple software baselines, version control, tracking unique updates to software builds, and conducting diffs of source code
- One (1) year experience in technical writing
- One (1) year experience with Waterfall software development life cycle concepts

#### **ADMINISTRATIVE ASSISTANT (01020):**

In addition to secretarial duties (filing, taking phone calls, scheduling appointments, making travel arrangements), this position will provide administrative support to executive staff with office management responsibilities to include budgeting, personnel records and payroll. The Administrative Assistant may be required to work independently on projects requiring research and preparation of briefing charts and other presentation materials.

**Minimum Education:** High School Diploma (or GED Equivalent)

**Minimum Experience:** Five (5) years of professional experience

#### **SPECIALIST INFORMATION SYSTEM SECURITY II (SISS2)**

The information System Security Specialist is responsible for supporting all aspects of a Program Information Assurance (IA) processes tailored to include minimum qualification standards, fundamental awareness and familiarity to demonstrated competency with specific experience in Cyber Security, Engineering, Test & Evaluation, (T&E) and/or Security Control Assessor (SCA) under a Certification & Accreditation (C&A) and/or Assessment & Authorization (A&A) process. The specialist should demonstrate a working knowledge of the Risk Management Framework (RMF) process and/or include prior experience with the Defense Information Assurance & Certification Accreditation Process (DIACAP). Familiarity with security policies & guidance documents to assist with the preparation and maintenance of process artifacts, traceability documents purposed for compliance with Authority to Operate (ATO) requirements. The specialist is expected to evaluate security solutions to ensure they meet security requirements for processing up to classified information, and supervise and/or maintain the operational security posture for an information system or program.

**Minimum Education:** High School Diploma or HS equivalency certificate

**Minimum Experience:** 2 Years of practical experience in a Cybersecurity, Engineering, T&E or A&A (formerly C&A) related field. Have worked with Information Assurance tools such as DISA Enterprise Mission Assurance Support Service (eMASS), Assured Compliance Assessment Solution (ACAS) and may be required to hold an Interim Security Control Assessor qualification.

-

#### **Information Assurance Functions and Personnel Requirements Note:**

Ensure that if you have any labor categories that will be performing Information Assurance (IA) Requirements including contractors who will be in the Cybersecurity (CS) workforce you must identify the required security, certifications, education, and training for EACH labor category. Reference DFARS Clause 252.239-7001, DoD 8750.01-M "Information Workforce Improvement Program", DoD 8140.01 "Cyberspace Workforce Management", and SECNAV M-5239.2 "Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual".

#### **9.6 DON Cyberspace IT (Information Technology) / Cybersecurity & Information Assurance Functions and Personnel Requirements**

**DoD IA Workforce DFARS Clause****252.239-7001 Information Assurance Contractor Training and Certification.**

As prescribed in [239.7103\(b\)](#), use the following clause:

**INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION**

(JAN 2008)

(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

(End of clause)

9.6.1 The table below outlines the requirements for the listed cyber positions:

Position	CSWF Label**	CSWF Proficiency**	IAT or IAM Level (1,2,3)	IAWF Baseline Requirements	Operating System/Computing Environment(OS/CE) Qualification	Continuing Professional Education (CPE) Requirements	IT Level (per SECNAV M-5510.30)
Analyst Computer Systems III	45	Advanced	IAT-3	CISSP or CASP or ENSA or Graduate Degree from accredited University or CNSSI or NTSSI 4015 or 4016	Directed by Privileged Access Agreement	40 CPE's Annually	3.11

Specialist Information System Security II	62	Advanced	IAT-3	Security + (CE) or CNSSI or NTSSI 4015 or 4016	Directed by Privileged Access Agreement	40 CPE's Annually	3.11
Analyst Computer System II	45	Intermediate/ Journeyman	IAT-2	GSEC or Security + (CE) or SSCP or  Bachelor Degree from accredited University or CNSSI or NTSSI 4015 or 4016	Directed by Privileged Access Agreement	40 CPE's Annually	3.11

**\*\* CSWF Label/CSWF Proficiency NOTE: See Appendix A for Additional Guidance** - These columns are for informational/planning purposes only. The current governing guidance is [DoDM 8570.01](#), Information Assurance. Workforce Improvement. Program. Per NAVADMIN 003/19, the Navy will be transitioning to [SECNAV M-5239.2](#) Department Of The Navy Cyberspace Information Technology And Cybersecurity Workforce Management And Qualification Manual. In efforts to facilitate that transition, the CSWF Label and CSWF Proficiency requirements column are provided (these are not applicable as of contract award date).

## 10.0 NSWCPD ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (ECRAFT) SYSTEM

10.1 In addition to the requirements of Clause C-237-W001 “Electronic Cost Reporting and Financial Tracking (eCRAFT) System Reporting (NAVSEA)”, the contractor is required to provide supporting accounting system reports, at the Contracting Officer’s request, based on the review of the invoice documentation submitted to eCRAFT. This documentation will include reports such as the Job Summary Report (or equivalent), Labor Distribution Report (or equivalent), and General Ledger Detail Report (or equivalent). Supporting labor data provided must include unburdened direct labor rates for each employee and labor category. Cost breakdowns for ODCs, Materials, travel and other non-labor costs must be at the transactional level in sufficient detail so the Government can review allocability to the contract/task order. Indirect costs allocated to direct costs must be shown at the lowest level of detail sufficient to reconcile each indirect rate to the appropriate allocation base.

10.2 On invoices containing subcontractor costs, the prime contractor agrees, at the Contracting Officer’s request, to attach as supporting documentation all invoices received from subcontractors, unless the subcontractor submits invoices directly to the CO and COR. This requirement applies to all subcontract types (Cost, FFP, etc.).

## 11.0 SPECIAL REQUIREMENTS

### 11.1 Quality Management System

11.1.1 The Contractor shall:

11.1.1.1. Maintain a Quality Management System (QMS) in accordance with ASQ/ANSI/ISO 9001:2015 standards per Naval Sea Systems Command (NAVSEA) QMS Acceptance Authority or appropriate directorate requirements. All QMS packages are required to adhere to applicable NAVSEA Technical Specification 9090-310 and NAVSEA Standard Item 009-04 requirements.

11.1.1.2. Notify NSWCPD’s Quality Department in writing when any changes are made to the QMS that may affect work defined in accordance with NAVSEA Technical Specification 9090-310.

11.1.1.3. Submit its QMS Level 3 specific work procedures relevant to the requirements of the Solicitation, including the SOW at the Task Order level (i.e. welding, etc.).

### 11.2 Risk Management

11.2.1. The contractor shall:

11.2.1.1. Develop an internal risk management program and work jointly with the Code 514 to develop an overall risk management program.

11.2.1.2. Assign responsibility for risk mitigation activities, and monitor progress through a formal tracking system.

11.2.1.3 Conduct risk identification and analysis during all phases of the program, including proposal development. Develop appropriate risk mitigation strategies and plans.

11.2.1.4. Use projected consequences of high probability risks to help establish the level of management reserve and schedule reserve.

11.2.1.5. Assess impact of identified performance, schedule and costs risks to estimate at completion, and include in the estimate as appropriate. Develop a range of estimates (best case, most likely, worst case).

11.2.1.6. The Contractor shall capture risks and associated mitigation plans in a risk database and provide status updates to the Government for all documented risks upon request.

**11.3. Minimum Standard Quality Contract Requirements for Material Procurement, Modification, Repair, or Overhaul of Material – Deep Submergence Systems – Scope of Certification MCD-A SMICs D5 & D6**

#### **Clauses Included by Full Text**

#### **C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)**

The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, Exhibit(s), attached hereto.

#### **C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)**

(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of \$1,000 or less at the time of final contract closeout. The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded. For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law.

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties. It is agreed that the administrative costs for either party associated with collecting such small dollar amounts could exceed the amount to be recovered.

#### **C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)**

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with detailed obligations to which the Contractor committed itself in Proposal N6449820R3042 dated 08/20/20 in response to NAVSEA Solicitation No. .

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52.215-8) clause of this contract. Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence.

#### **C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)**

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as "protected information". File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

- (1) The support contractor not disclose any information;
- (2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files.
- (3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,
- (4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, or any person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

#### **C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)**

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employee's name, work site, and contract number.

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state

and local requirements while in

Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractor's injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required. (d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(e) The Safety Office points of contacts are as follows: Paul Breeden (paul.breeden@navy.mil) and Al D'Imperio (albert.dimperio@navy.mil).

#### C-237-H001 SERVICE CONTRACT REPORTING (NAVSEA) (JAN 2021)

(a) Services Contract Reporting (SCR) requirements apply to this contract. The contractor shall report required SCR data fields using the SCR section of the System for Award Management (SAM) at following web address: <https://sam.gov/SAM/>.

(b) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at <https://sam.gov/SAM/>.

#### C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed. Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract. No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement. Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel.

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Contracting Officer shall be notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include:

(1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

#### C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (MAY 2019)

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting and Financial Tracking (eCRAFT) System and submit the Contractor's Performance Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination.

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks. It informs the Government of existing or potential problem areas.

(c) The Contractor's Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges.

(1) Access: eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU). The EPRU spreadsheet and user manual can be obtained at: <http://www.navsea.navy.mil/Home/Warfare-Centers/NUWC-Newport/Partnerships/Commercial-Contracts/Information-eCraft/> under eCRAFT information. The link for eCRAFT report submission is: [https://www.pdrep.csd.disa.mil/pdrep\\_files/other/ecraft.htm](https://www.pdrep.csd.disa.mil/pdrep_files/other/ecraft.htm). If you have problems uploading reports, please see the Frequently Asked Questions at the site address above.

(2) Submission and Acceptance/Rejection: Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in WAWF. The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT.

#### C-242-H002 POST AWARD MEETNG (NAVSEA) (OCT 2018)

(a) A post-award meeting with the successful offeror will be conducted within [ \* ] days after award of the Task Order. The meeting will be held at the address below: Location/Address: [ \* ]

(b) The contractor will be given [ \* ] working days notice prior to the date of the meeting by the Contracting Officer.

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the [contract / task order].

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out. Specific topics shall be mutually agreed to prior to the meeting.

[ \* ] To be specified at Task Order award

#### **C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)**

(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

#### **C-227-H008 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (NAVSEA) (DEC 2018)**

(a) The contractor shall actively participate in the Government Industry Data Exchange Program in accordance with the GIDEP Operations Manual, S0300-BT-PRO-010. The contractor shall submit information concerning critical or major nonconformances, as defined in FAR 46.407/DFARS 246.407, to the GIDEP information system.

(b) The contractor shall insert paragraph (a) of this clause in any subcontract when deemed necessary. When so inserted, the word "contractor" shall be change to "subcontractor."

(c) The contractor shall, when it elects not to insert paragraph (a) in a subcontract, provide the subcontractor any GIDEP data which may be pertinent to items of its manufacture and verify that the subcontractor utilizes any such data.

(d) The contractor shall, whether it elects to insert paragraph (a) in a subcontract or not, verify that the subcontractor utilizes and provides feedback on any GIDEP data that may be pertinent to items of its manufacture."

(e) GIDEP materials, software and information are available without charge from: GIDEP Operations Center

P.O. Box 8000

Corona, CA 92878-8000

Phone: (951) 898-3207

FAX: (951) 898-3250

Internet: <http://www.gidep.org>

#### **C-244-H002 SUBCONTRACTORS/CONSULTANTS (NAVSEA) (OCT 2018)**

Notwithstanding FAR 52.244-2(d) and in addition to the information required by FAR 52.244-2(e) of the contract, the contractor shall include the following information in requests to add subcontractors or consultants during performance, regardless of subcontract type or pricing arrangement:

(1) Impact on subcontracting goals,

(2) Impact on providing support at the contracted value,

(3) IF SEAPORT TASK ORDER - The results of negotiations to incorporate fee rate caps no higher than the lower of (i) SeaPort fee rate caps for the prime contractor, or in the case where the proposed subcontractor is also a SeaPort prime, (ii) fee rate caps that are no higher than the subcontractor's prime SeaPort contract.